3

Coordinatisation of projective spaces

In this chapter, we describe axiom systems for projective (and affine) spaces. The principal results are due to Veblen and Young.

3.1 The $\mathrm{GF}(2)$ case

In the last section, we saw an axiomatic characterisation of the geometries $\mathrm{PG}(2,F)$ (as projective planes satisfying Desargues' Theorem). We turn now to the characterisation of projective spaces of arbitrary dimension, due to Veblen and Young. Since the points and the subspaces of any fixed dimension determine the geometry, we expect an axiomatisation in terms of these. Obviously the case of points and lines will be the simplest.

For the first of several times in these notes, we will give a detailed and self-contained argument for the case of $\mathrm{GF}(2)$, and treat the general case in rather less detail.

Theorem 3.1 *Let X be a set of points, $\mathcal{L}$ a set of subsets of X called lines. Assume:*

(a) any two points lie on a unique line;

(b) a line meeting two sides of a triangle, not at a vertex, meets the third side;

(c) a line contains exactly three points.

Then X and $\mathcal{L}$ are the sets of points and lines in a (not necessarily finite dimensional) projective space over $\mathrm{GF}(2)$.

htb

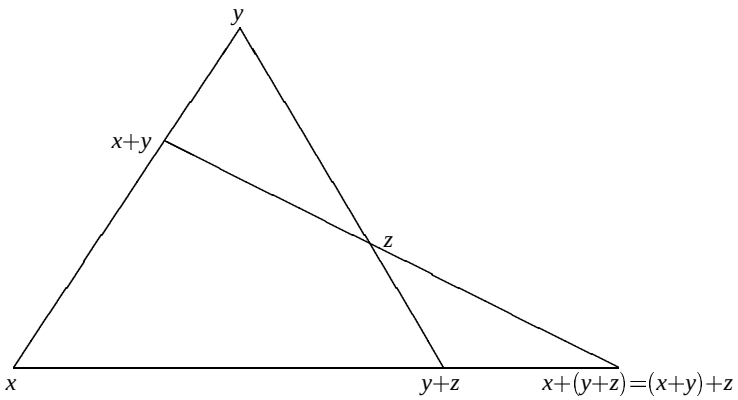

Figure 3.1: Veblen's Axiom

Remark We will see later that, more or less, conditions (a) and (b) characterise arbitrary projective spaces. Condition (c) obviously specifies that the field is GF(2). The phrase "not necessarily finite dimensional" should be interpreted as meaning that X and $\mathcal{L}$ can be identified with the subspaces of rank 1 and 2 respectively of a vector space over GF(2), not necessarily of finite rank.

Proof Since 1 is the only non-zero scalar in GF(2), the points of projective space can be identified with the non-zero vectors; lines are then triples of non-zero vectors with sum 0. Our job is to reconstruct this space.

Let 0 be an element not in X, and set $V = X \cup \{0\}$. Now define an addition in V as follows:

- for all $v \in V$, $0+v = v+0 = v$ and $v+v = 0$;
- for all $x,y \in X$ with $x \neq y$, $x+y = z$, where z is the third point of the line containing x and y.

We claim that $(V,+)$ is an abelian group. Commutativity is clear; 0 is the identity, and each element is its own inverse. Only the associative law is non-trivial; and the only non-trivial case, when x,y,z are distinct non-collinear points, follows immediately from Veblen's axiom (b) (see Fig. 3.1.1).

Next, we define scalar multiplication over GF(2), in the only possible way: $0 \cdot v = 0$, $1 \cdot v = v$ for all $v \in V$. The only non-trivial vector space axiom is $(1+1) \cdot v = 1 \cdot v + 1 \cdot v$, and this follows from $v+v = 0$.

Finally, $\{0,x,y,z\}$ is a rank 2 subspace if and only if $x+y = z$.

There is a different but even simpler characterisation in terms of hyperplanes, which foreshadows some later developments.

Let $\mathcal{L}$ be any family of subsets of X. The subset Y of X is called a *subspace* if any member of $\mathcal{L}$ which contains two points of Y is wholly contained within Y. (Thus, the empty set, the whole of X, and any singleton are trivially subspaces.) The subspace Y is called a *hyperplane* if it intersects every member of $\mathcal{L}$ (necessarily in one or all of its points).

Theorem 3.2 *Let $\mathcal{L}$ be a collection of subsets of X. Suppose that*

(a) every set in $\mathcal{L}$ has cardinality 3;

(b) any two points of X lie in at least one member of $\mathcal{L}$;

(c) every point of X lies outside some hyperplane.

Then X and $\mathcal{L}$ are the point and line sets of a projective geometry over GF(2)*, not necessarily finite dimensional.*

Proof Let $\mathcal{H}$ be the set of hyperplanes. For each point $x \in X$, we define a function $p_x : \mathcal{H} \to \mathrm{GF}(2)$ by the rule

$$p_x(H) = \begin{cases} 0 & \text{if } x \in H; \\ 1 & \text{if } x \notin H. \end{cases}$$

By condition (c), p_x is non-zero for all $x \in X$.

Let $P = \{p_x : x \in X\}$. We claim that $P \cup \{0\}$ is a subspace of the vector space $\mathrm{GF}(2)^{\mathcal{H}}$ of functions from $\mathcal{H}$ to GF(2). Take $x, y \in X$, and let $\{x, y, z\}$ be any set in $\mathcal{L}$ containing x and y. Then a hyperplane contains z if and only if it contains both or neither of x and y; so $p_z = p_x + p_y$. The claim follows.

Now the map $x \mapsto p_x$ is 1–1, since if $p_x = p_y$ then $p_x + p_y = 0$, contradicting the preceding paragraph. Clearly this map takes members of $\mathcal{L}$ to lines. The theorem is proved.

Remark The fact that two points lie in a unique line turns out to be a consequence of the other assumptions.

Exercises

1. Suppose that conditions (a) and (c) of Theorem 3.1.2 hold. Prove that two points of X lie in at most one member of $\mathcal{L}$.

2. Let $(X, \mathcal{L})$ satisfy conditions (a) and (c) of Theorem 3.1.1. Let Y be the set of points x of X with the following property: for any two lines $\{x, y_1, y_2\}$ and $\{x, z_1, z_2\}$ containing x, the lines y_1z_1 and y_2z_2 intersect. Prove that Y is a subspace of X.

3. Let X be a set of points, $\mathcal{B}$ a collection of subsets of X called lines. Assume that any two points lie in at least one line, and that every point lies outside some hyperplane. Show that, if the line size is not restricted to be 3, then we cannot conclude that X and $\mathcal{B}$ are the point and line sets of a projective space, even if any two points lie on exactly one line. [Hint: In a projective plane, any line is a hyperplane. Select three lines L_1, L_2, L_3 forming a triangle. Show that it is possible to delete some points, and to add some lines, so that L_1, L_2, L_3 remain hyperplanes.]

4. Let $(X, \mathcal{B})$ satisfy the hypotheses of the previous question. Assume additionally that any two points lie on a unique line, and that some hyperplane is a line and is finite. Prove that there is a number n such that any hyperplane contains $n+1$ points, any point lies on $n+1$ lines, and the total number of lines is n^2+n+1.

3.2 An application

I now give a brief application to coding theory. This application is a bit spurious, since a more general result can be proved by a different but equally simple argument; but it demonstrates an important link between these fields. Additionally, the procedure can be reversed, to give characterisations of other combinatorial designs using theorems about codes.

The problem tackled by the theory of error-correcting codes is to send a message over a noisy channel in which some distortion may occur, so that the errors can be corrected but the price paid in loss of speed is not too great. This is not the place to discuss coding theory in detail. We simplify by assuming that a message transmitted over the channel is a sequence of blocks, each block being an n-tuple of *bits* (zeros or ones). We also assume that we can be confident that, during the transmission of a single block, no more than e bits are transmitted incorrectly (a zero changed to a one or *vice versa*). The *Hamming distance* between two blocks is the number of coordinates in which they differ; that is, the number of errors required to change one into the other. A *code* is just a set of "codewords" or blocks (n-tuples of bits), containing more than one codeword. It is *e-error correcting* if the Hamming distance between two codewords is at least $2e+1$. (The reason for the name is that, by the triangle inequality, an arbitrary word cannot lie at distance

e or less from more than one codeword. By our assumption, the received word lies at distance e or less from the transmitted codeword; so this codeword can be recovered.)

To maximise the transmission rate, we need as many codewords as possible. The optimum is obtained when every word lies within distance e of a (unique) codeword. In other words, the closed balls of radius e centred at the codewords fill the space of all words without any overlap! A code with this property is called *perfect e-error-correcting*.

Encoding and decoding are made much easier if the code is *linear*, that is, it is a $\mathrm{GF}(2)$-subspace of the vector space $\mathrm{GF}(2)^n$ of all words.

Theorem 3.3 *A linear perfect* 1*-error-correcting code has length* $2^d - 1$ *for some* $d > 1$*; there is a unique such code of any length having this form.*

Remark These unique codes are called *Hamming codes*. Their relation to projective spaces will be made clear by the proof below.

Proof Let C be such a code, of length n. Obviously it contains $\mathbf{0}$. We define the *weight* $\mathrm{wt}(\mathbf{v})$ of any word $\mathbf{v}$ to be its Hamming distance from $\mathbf{0}$. The weight of any non-zero codeword is at least 3. Now let X be the set of coordinate places, and $\mathcal{L}$ the set of triples of points of X which support codewords (i.e., for which a codeword has 1s in just those positions).

We verify the hypotheses of Theorem 3.1. Condition (c) is clear.

Let x and y be coordinate positions, and let $\mathbf{w}$ be the word with entries 1 in positions x and y and 0 elsewhere. $\mathbf{w}$ is not a codeword, so there must be a unique codeword $\mathbf{c}$ at distance 1 from $\mathbf{w}$; then $\mathbf{c}$ must have weight 3 and support containing x and y. So (a) holds.

Let $\{x,y,r\},\{x,z,q\},\{y,z,p\}$ be the supports of codewords $\mathbf{u},\mathbf{v},\mathbf{w}$. By linearity, $\mathbf{u}+\mathbf{v}+\mathbf{w}$ is a codeword, and its support is $\{p,q,r\}$. So (b) holds.

Thus X and $\mathcal{L}$ are the points and lines of a projective space $\mathrm{PG}(d-1,2)$ for some $d > 1$; the number of points is $n = 2^d - 1$. Moreover, it's easy to see that C is spanned by its words of weight 3 (see Exercise 1), so it is uniquely determined by d.

Note, incidentally, that the automorphism group of the Hamming code is the same as that of the projective space, viz. $\mathrm{PGL}(d,2)$.

Exercise

1. Prove that a perfect linear code is spanned by its words of minimum weight. (Use induction on the weight. If $\mathbf{w}$ is any non-zero codeword, there is a codeword $\mathbf{u}$ whose support contains $e+1$ points of the support of $\mathbf{w}$; then $\mathbf{u}+\mathbf{w}$ has smaller weight than $\mathbf{w}$.)

2. Prove that if a perfect e-error-correcting code of length n exists, then

$$\sum_{i=0}^{e} \binom{n}{i}$$

is a power of 2. Deduce that, if $e = 3$, then $n = 7$ or 23. (Hint: the cubic polynomial in n factorises.)

Remark. The case $n = 7$ is trivial. For $n = 23$, there is a unique code (up to isometry), the so-called *binary Golay code*.

3. Verify the following decoding scheme for the Hamming code H_d of length $2^d - 1$. Let M_d be the $2^d - 1 \times d$ matrix over GF(2) whose rows are the base 2 representations of the integers $1, 2, \ldots, 2^d - 1$. Show that the null space of the matrix M_d is precisely H_d. Now let $\mathbf{w}$ be received when a codeword is transmitted, and assume that at most one error has occurred. Prove that

- if $\mathbf{w}H_d = 0$, then $\mathbf{w}$ is correct;
- if $\mathbf{w}H_d$ is the i^{th} row of H_d, then the i^{th} position is incorrect.

3.3 The general case

The general coordinatisation theorem is the same as Theorem 3.1, with the hypothesis "three points per line" weakened to "at least three points per line". Accordingly we consider geometries with point set X and line set $\mathcal{L}$ (where $\mathcal{L}$ is a set of subsets of X) satisfying:

(LS1) Any line contains at least two points.

(LS2) Two points lie in a unique line.

Such a geometry is called a *linear space*. Recall that a subspace is a set of points which contains the (unique) line through any two of its points. In a linear space, in addition to the trivial subspaces (the empty set, singletons, and X), any line is

a subspace. Any subspace, equipped with the lines it contains, is a linear space in its own right.

A linear space is called *thick* if it satisfies:

(LS1+) Any line contains at least three points.

Finally, we will impose Veblen's Axiom:

(V) A line meeting two sides of a triangle, not at a vertex, meets the third side also.

Theorem 3.4 (Veblen–Young Theorem) *Let $(X, \mathcal{L})$ be a linear space, which is thick and satisfies Veblen's Axiom (V). Then one of the following holds:*

(a) $X = \mathcal{L} = \emptyset$*;*

(b) $|X| = 1$, $\mathcal{L} = \emptyset$*;*

(c) $\mathcal{L} = \{X\}$, $|X| \geq 3$*;*

(d) $(X, \mathcal{L})$ *is a projective plane;*

(e) $(X, \mathcal{L})$ *is a projective space over a skew field, not necessarily of finite dimension.*

Remark It is common to restrict to finite-dimensional projective spaces by adding the additional hypothesis that any chain of subspaces has finite length.

Proof (outline) The key observation provides us with lots of subspaces.

Lemma 3.5 *Let $(X, \mathcal{L})$ be a linear space satisfying Veblen's axiom. Let Y be a subspace, and p a point not in Y; let Z be the union of the lines joining p to points of Y. Then Z is a subspace, and Y is a hyperplane in Z.*

Proof Let q and r be points of Z. There are several cases, of which the generic case is that where $q, r \notin Y$ and the lines pq and pr meet Y in distinct points s, t. By (V), the lines qr and st meet at a point u of Y. If v is another point of qr, then by (V) again, the line pv meets st at a point of Y; so $v \in Z$.

We write this subspace as $\langle Y, p\rangle$.

Now, if L is a line and p a point not in L, then $\langle L, p\rangle$ is a projective plane. (It is a subspace in which L is a hyperplane; all that has to be shown is that every line is a hyperplane, which follows once we show that $\langle L, p\rangle$ contains no proper subspace properly containing a line.)

The theorem is clearly true if there do not exist four non-coplanar points; so we may suppose that such points do exist.

We claim that Desargues' Theorem holds. To see this examine the geometric proof of Desargues' Theorem in Section 1.2; it is obvious for any non-planar configuration, and the planar case follows by several applications of the non-planar case. Now the same argument applies here.

It follows from Theorem 2.1 that every plane in our space can be coordinatised by a skew field.

To complete the proof, we have to show that the coordinatisation can be extended consistently to the whole space. For this, first one shows that the skew fields coordinatising all planes are the same: this can be proved for planes within a 3-dimensional subspace by means of central collineations, and the result extends by connectedness to all pairs of planes. The remainder of the argument involves careful book-keeping.

From this, we can find a classification of not necessarily thick linear spaces satisfying Veblen's axiom. The *sum* of a family of linear spaces is defined as follows. The point set is the disjoint union of the point sets of the constituent spaces. Lines are of two types:

(a) all lines of the constituent spaces;

(b) all pairs of points from different constituents.

It is clearly a linear space.

Theorem 3.6 *A linear space satisfying Veblen's axiom is the sum of linear spaces of types (b)–(e) in the conclusion of Theorem 3.4.*

Proof Let $(X, \mathcal{L})$ be such a space. Define a relation $\sim$ on X by the rule that $x \sim y$ if either $x = y$, or the line containing x and y is thick (has at least three points). We claim first that $\sim$ is an equivalence relation. Reflexivity and symmetry are clear; so assume that $x \sim y$ and $y \sim z$, where we may assume that x, y and z are all distinct. If these points are collinear, then $x \sim z$; so suppose not; let x_1 and z_1 be

further points on the lines xy and yz respectively. By (V), the line x_1z_1 contains a point of xz different from x and z, as required.

So X is the disjoint union of equivalence classes. We show next that any equivalence class is a subspace. So let $x \sim y$. Then $x \sim z$ for every point z of the line xy; so this line is contained in the equivalence class of x.

So each equivalence class is a non-empty thick linear space, and hence a point, line, projective plane, or projective space over a skew field, by Theorem 3.4. It is clear that the whole space is the sum of its components.

A geometry satisfying the conclusion of Theorem 3.6 is called a *generalised projective space*. Its flats are its (linear) subspaces; these are precisely the sums of flats of the components. The term "projective space" is sometimes extended to mean "thick generalised projective space" (i.e., to include single points, lines with at least three points, and not necessarily Desarguesian projective planes).

3.4 Lattices

Another point of view is to regard the flats of a projective space as forming a lattice. We discuss this in the present section.

A *lattice* is a set L with two binary operations $\vee$ and $\wedge$ (called *join* and *meet*), and two constants 0 and 1, satisfying the following axioms:

(L1) $\vee$ and $\wedge$ are idempotent, commutative, and associative;

(L2) $x \vee (x \wedge y) = x$ and $x \wedge (x \vee y) = x$;

(L3) $x \wedge 0 = x$, $x \vee 1 = x$.

It follows from these axioms that $x \wedge y = x$ holds if and only if $x \vee y = y$ holds. We write $x \leq y$ if these equivalent conditions hold. Then $(L, \leq)$ is a partially ordered set with greatest element 1 and least element 0; $x \vee y$ and $x \wedge y$ are the least upper bound and greatest lower bound of x and y respectively. Conversely, any partially ordered set in which least upper bounds and greatest lower bounds of all pairs of elements exist, and there is a least element and a greatest element, gives rise to a lattice.

In a lattice, an *atom* is a non-zero element a such that $a \wedge x = 0$ or a for any x; in other words, an element greater than zero but minimal subject to this. The lattice is called *atomic* if every element is a join of atoms.

A lattice is *modular* if it satisfies:

(M) If $x \leq z$, then $x \vee (y \wedge z) = (x \vee y) \wedge z$ for all y.

(Note that, if $x \leq z$, then $x \vee (y \wedge z) \leq (x \vee y) \wedge z$ in any lattice.)

Theorem 3.7 *A lattice is a generalised projective space of finite dimension if and only if it is atomic and modular.*

Proof The forward implication is an exercise. Suppose that the lattice L is atomic and modular. Let X be the set of atoms. Identify every element z of the lattice with the set $\{x \in X : x \leq z\}$. (This map is 1–1; it translates meets to intersections, and the lattice order to the inclusion order.)

Let x, y, z be atoms, and suppose that $z \leq x \vee y$. Then trivially $x \vee z \leq x \vee y$. Suppose that these two elements are unequal. Then $y \not\leq x \vee z$. Since y is an atom, $y \wedge (x \vee z) = 0$, and so $x \vee (y \wedge (x \vee z)) = x$. But $(x \vee y) \wedge (x \vee z) = x \vee z$, contradicting modularity. So $x \vee z = x \vee y$. Hence, if we define lines to be joins of pairs of atoms, it follows that two points lie in a unique line.

Now we demonstrate Veblen's axiom. Let u, v be points on $x \vee y$, $x \vee z$ respectively, where xyz is a triangle. Suppose that $(y \vee z) \wedge (u \vee v) = 0$. Then $y \vee u \vee v \geq z$, so $y \vee u \vee v \geq y \vee z$; in other words, $y \vee (u \vee v)) \wedge (y \vee z) = y \vee z$. On the other hand, $y \vee ((u \vee v) \wedge (y \vee z)) = y \vee 0 = y$, contradicting modularity. So the lines $y \vee z$ and $u \vee v$ meet.

By Theorem 3.6, the linear subspace is a generalised projective geometry. Clearly the geometry has finite dimension. We leave it as an exercise to show that every flat of the geometry is an element of the lattice.

Exercises

1. Complete the proof of Theorem 3.7.
2. Show that an atomic lattice satisfying the distributive laws is modular, and deduce that it is isomorphic to the lattice of subsets of a finite set.

3.5 Affine spaces

Veblen's axiom in a linear space is equivalent to the assertion that three non-collinear points lie in a subspace which is a projective plane. It might be hoped that replacing "projective plane" by "affine plane" here would give an axiomatisation of affine spaces. We will see that this is almost true.

Recall from Section 2.1 the definition of an affine plane, and the fact that parallelism is an equivalence relation in an affine plane, where two lines are parallel if they are equal or disjoint.

Now suppose that $(X, \mathcal{L})$ is a linear space satisfying the following condition:

(AS1) There is a collection $\mathcal{A}$ of subspaces with the properties that each member of $\mathcal{A}$ is an affine plane, and that any three non-collinear points are contained in a unique member of $\mathcal{A}$.

First, a few remarks about such spaces.

1. All lines have the same cardinality. For two intersecting lines lie in an affine plane, and so are equicardinal; and, given two disjoint lines, there is a line meeting both.

2. It would be simpler to say "any three points generate an affine plane", where the subspace *generated by* a set is the intersection of all subspaces containing it. This formulation is equivalent if the cardinality of a line is not 2. (Affine spaces of order greater than 2 have no non-trivial proper subspaces.) But, if lines have cardinality 2, then any pair of points is a line, and so any three points form a subspace which is a generalised projective plane. However, we do want a formulation which includes this case.

3. In a linear space satisfying (AS1), two lines are said to be *parallel* if either they are equal, or they are disjoint and contained in a member of $\mathcal{A}$ (and hence parallel there). Now Playfair's Axiom holds: given a line L and point p, there is a unique line parallel to L and containing p. Moreover, parallelism is reflexive and symmetric, but not necessarily transitive. We will impose the further condition:

(AS2) Parallelism is transitive.

Theorem 3.8 *A linear space satisfying (AS1) and (AS2) is empty, a single point, a single line, an affine plane, or the configuration of points and lines in a (not necessarily finite-dimensional) affine space.*

Proof Let $(X, \mathcal{L})$ be the linear space. We may assume that it is not empty, a point, a line, or an affine plane (i.e., that there exist four non-coplanar points).

Step 1. Define a *solid* to be the union of all the lines in a parallel class C which meet a plane $\Pi \in \mathcal{A}$, where Π contains no line of C. Then any four non-coplanar points lie in a unique solid, and any solid is a subspace.

That a solid is a subspace is shown by considering cases, of which the generic one runs as follows. Let p, q be points such that the lines of C containing p and q meet Π in distinct points x and y. Then x, y, p, q lie in an affine plane; so the line of C through a point r of pq meets Π in a point x of xy.

Now the fact that the solid is determined by any four non-coplanar points follows by showing that it has no non-trivial proper subspaces except planes (if the cardinality of a line is not 2) or by counting (otherwise).

In a solid, if a plane Π contains no parallel to a line L, then Π meets L in a single point. Hence any two planes in a solid are disjoint or meet in a line.

Step 2. If two planes Π and Π' contain lines from two different parallel classes, then every line of Π is parallel to a line of Π'.

Suppose not, and let L, M, N be lines of Π, concurrent at p, and p' a point of Π' such that the lines L', M' through p' parallel to L and M lie in Π', but the line N' parallel to N does not. The whole configuration lies in a solid; so the planes NN' and Π', with a common point p', meet in a line K. Now K is coplanar with N but not parallel to it, so $K \cap N$ is a point q. Then Π and Π' meet in q, and hence in a line J. But then J is parallel to both L and M, a contradiction.

We call two such planes *parallel*.

Step 3. We build the embedding projective space. Here I will use a typographic convention to distinguish the two related spaces: elements of the space we are building will be written in CAPITALS. The POINTS are the points of X and the parallel classes of lines of $\mathcal{A}$. The LINES are the lines of $\mathcal{L}$ and the parallel classes of planes in $\mathcal{A}$. Incidence is hopefully obvious: as in the old space, together with incidence between any line and its parallel class, as well as between a parallel class C of lines and a parallel class $\mathcal{C}$ of planes if a plane in $\mathcal{C}$ contains a line in C.

By Step 2, this is a linear space; and clearly every LINE contains at least three POINTS. We call the new POINTS and LINES (i.e., the parallel classes) "ideal".

Step 4. We verify Veblen's Axiom. Any three points which are not all "ideal" lie in an affine plane with its points at infinity adjoined, i.e., a projective plane. So let pqr be a triangle of "ideal" POINTS, s and t POINTS on pq and pr respectively, and o a point of X. Let P, Q, R, S, T be the lines through o in the parallel classes p, q, r, s, t respectively. Then these five lines lie in a solid, so the planes QR and ST (having the point o in common) meet in a line u. The parallel class U of u is the required POINT on qr and st.

By Theorem 3.4, the extended geometry is a projective space. The points at infinity obviously form a hyperplane, and so the original points and lines form an affine space.

We spell the result out in the case where lines have cardinality 2, but referring only to parallelism, not to the planes.

Corollary 3.9 *Suppose that the 2-element subsets of a set X are partitioned into "parallel classes" so that each class partitions X. Suppose that, for any four points $p,q,r,s \in X$, if $pq \parallel rs$, then $pr \parallel qs$. Then the points and parallelism are those of an affine space over* $\mathrm{GF}(2)$.

Here, we have used the notation $\parallel$ to mean "belong to the same parallel class as". The result follows immediately from the theorem, on defining $\mathcal{A}$ to be the set of 4-element subsets which are the union of two parallel 2-subsets.

Exercises

1. Give a direct proof of the Corollary, in the spirit of Section 3.1.

3.6 Transitivity of parallelism

A remarkable theorem of Buekenhout [6] shows that it is not necessary to assume axiom (AS2) (the transitivity of parallelism) in Theorem 3.8, provided that the cardinality of a line is at least 4. Examples due to Hall [19] show that the condition really is needed if lines have cardinality 3.

Theorem 3.10 *Let $(X,\mathcal{L})$ be a linear space satisfying (AS1), in which some line contains at least four points. Then parallelism is transitive (that is, (AS2) holds), and so $(X,\mathcal{L})$ is an affine space.*

To discuss the counterexamples with 2 or 3 points on a line, some terminology is helpful. A *Steiner triple system* is a collection of 3-subsets of a set, any two points lying in a unique subset of the collection. In other words, it is a linear space with all lines of cardinality 3, or (in the terminology of Section 1.4) a 2-$(v,3,1)$ design for some (possibly infinite) v. A *Steiner quadruple system* is a set of 4-subsets of a set, any three points in a unique subset in the collection (that is, a 3-$(v,4,1)$ design.)

A linear space satisfying (AS1), with two points per line, is equivalent to a Steiner quadruple system: the distinguished 4-sets are the affine planes. There are Steiner quadruple systems aplenty; most are not affine spaces over $\mathrm{GF}(2)$ (for example, because the number of points is not a power of 2). Here is an example. Let $A = \{1,2,3,4,5,6\}$. Let X be the set of all partitions of A into two sets of size 3 (so that $|X| = 10$). Define two types of 4-subsets of X:

(a) for all $a, b \in A$, the set of partitions for which a, b lie in the same part;

(b) for all partitions of A into three 2-sets A_1, A_2, A_3, the set of all partitions into two 3-sets each of which is a transversal to the three sets A_i.

This is a Steiner quadruple system with 10 points.

In the case of three points per line, we have the following result, for which we refer to Bruck [D] and Hall [18, 19]:

Theorem 3.11 *(a) In a finite Steiner triple system satisfying (AS1), the number of points is a power of* 3.

(b) For every $d \geq 4$, there is a Steiner triple system with 3^d points which is not isomorphic to $\mathrm{AG}(d,3)$.

Exercises

1. Prove that the number of points in a Steiner triple system is either 0 or congruent to 1 or 3 (mod 6), while the number of points in a Steiner quadruple system is 0, 1, or congruent to 2 or 4 (mod 6).

(It is known that these conditions are sufficient for the existence of Steiner triple and quadruple systems.)

2. Let $(X, \mathcal{L})$ be a Steiner triple system satisfying (AS1). For each point $x \in X$, let τ_x be the permutation of X which fixes x and interchanges y and z whenever $\{x,y,z\}$ is a triple. Prove that

(a) τ_x is an automorphism;

(b) $\tau_x^2 = 1$;

(c) for $x \neq y$, $(\tau_x \tau_y)^3 = 1$.